UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/879,575	06/12/2001	James Alexander Reeds III	1999-0275	4755

34700 7590 01/27/2005

DOCKET CLERK
P.O. BOX 802432
DALLAS, TX 75380

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/879,575	REEDS ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *Jun'01 & Apr'03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 12 June 2001.

2. Claims 1-53 are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 33-48 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claim 33 is directed to a receiver comprising: "a session count evaluator configured" and "a decryption engine configured". The terminology used as well as the description in the specification indicates that the session count evaluator and the decryption engine are nothing more than a computer program or software. Likewise independent claim 41 is directed to a transmitter ... comprising: "an encryption engine configured" and a "session count generator configured". The terminology used as well as the description in the specification indicates that the encryption engine and the session count generator are nothing more than a computer program. In addition independent claim 48 is directed to a system with the transmitter and receiver "configured" with the same terminology as claims 33 and 41 combined.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 2-13 rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. In claim 2 the text indicates: "wherein the applying comprises ... encryption process" whereas in the independent claim 1 the text indicates: "decrypting a payload of the data packet by applying".

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 4, 17, 25-32, 36, and 44 contain the trademark/trade name "RC4" owned by RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a proprietary standard for stream cipher and, accordingly, the identification/description is indefinite.

9. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 1-5, 14-17, 41-44, 49, and 53** are rejected under 35 U.S.C. 102(e) as being anticipated by Klingler et al. U.S. Patent Application Publication No. 2003/0003896 (hereinafter '896).

As to independent claim 1, "A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is taught in '896 page 3, paragraphs 0043-0046.

As to dependent claim 2, "wherein the applying comprises performing a bit per bit streaming encryption process" is shown in '896 page 3, paragraph 0041.

As to dependent claim 3, "wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet" is disclosed in '896 page 8, paragraph 0102.

As to dependent claim 4, "wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet" is taught in '896 page 4 paragraphs 0055-0057.

As to dependent claim 5. A method in accordance with claim 2, further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count" is shown in '896 paragraphs 0082.

As to dependent claim 6, "wherein the data packet further comprises at least a portion of a received message digest value" is disclosed in '896 page 3, paragraph 0039.

As to dependent claim 7 "wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value" is disclosed in '896 page 8, paragraph 0102.

As to dependent claim 8, "wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count" is taught in '896 pages 7 through 8, paragraphs 0093-0104.

As to dependent claim 9, "further comprising: discarding the data packet if the difference is not less than the threshold value" is shown in '896 page 8, paragraph 0103.

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value" is disclosed in '896 page 7, paragraphs 0091-0092.

As to dependent claim 11, "further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value" is taught in '896 page 3, paragraphs 0039-0040.

As to dependent claim 12, "further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value" is shown in '896 page 3, paragraph 0043.

As to dependent claim 13, "further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value" is disclosed in '896 page 4, paragraphs 0058-0060..

As to independent claim 14, "A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream; applying a portion of the fixed length segment to data to form an encrypted payload; generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" is taught in '896 page 3, paragraphs 0043-0046.

As to dependent claims 15, 16, and 17, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claim 18, "further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet" is taught in '896 page 3, paragraphs 0039-0040.

As to dependent claim 19, A method in accordance with claim 18, wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key" is shown in '896 page 3, paragraphs 0039-0041.

As to dependent claim 20, "further comprising: forming the at least a portion of the message digest value by truncating the message digest value" is disclosed in '896 page 4, paragraphs 0058-0060.

As to dependent claim 21, "further comprising transmitting the encrypted data packet to a receiver through a communication channel" is taught in '896 page 3, paragraphs 0034-0035.

As to independent claim 22, "further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is shown in '896 pages 7 through 8, paragraphs 0093-0104.

As to dependent claims 23, 24, and 25, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claims 26-32, these claims contain substantially similar subject matter as claims 7-13; therefore they are rejected along the same rationale.

As to independent claim 33, "A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received

encrypted data packet and a locally generated session count is less than a threshold; and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold" is taught in '896 page 3, paragraphs 0043-0046.

As to dependent claims 34-40 these claims contain substantially similar subject matter as claims 2-13; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42, 43, and 44, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claims 45, 46, and 47, these claims contain substantially similar subject matter as claims 18, 19, and 20; therefore they are rejected along the same rationale.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to independent claim 49, "A method comprising: receiving a data packet through a communication channel; the data packet comprising at least a portion of a session count; selecting a fixed length segment of a continuous decryption key stream based on the session count; and applying a portion of the fixed length segment by performing a bit per bit streaming encryption to decrypt a payload of the data packet" is taught in '896 page 3, paragraphs 0043-0046.

As to dependent claims 50, 51, and 52, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to independent claim 53, **"A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream; applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload; generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet"** is taught in '896 page 3, paragraphs 0043-0046

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Staring	U.S. Patent Application Publication No. 2001/0007127	
Carroll et al.	U.S. Patent Application Publication No. 2002/0006197	
Wee et al.	U.S. Patent Application Publication No. 2002/0164018	
Sharma et al.	U.S. Patent No. 6,778,670	issued 17 August 2004
Urban et al.	U.S. Patent No. 6,587,441	issued 1 July 2003
Rose et al.	U.S. Patent No. 6,560,338	issued 6 May 2003
Ellis	U.S. Patent No. 6,484,257	issued 19 November 2002
Reeds, III	U.S. Patent No. 5,727,064	issued 10 March 1998

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
10 January 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2134